FILED
2024 Jul-23 PM 03:16
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
NORTHERN DIVISION

JANE DOE as mother and next friend of MARY DOE, on behalf of herself and all others who are similarly situated,	)	
Plaintiffs,	)	**CIVIL ACTION NO.: _____**
v.	)	
TICKETMASTER, LLC., and LIVE NATION WORLDWIDE, INC.	)	
Defendant.	)	

COMPLAINT

Plaintiff Jane Doe as mother and next friend of Mary Doe, individually, and on behalf of all others similarly situated, bring this Class Action Complaint, and allege the following against Defendants Ticketmaster LLC, ("Ticketmaster"), and Live Nation Worldwide Inc., ("Live Nation") and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information **("PII")**, including but not limited to "full names, addresses, email addresses, phone numbers, tickets sales and event details, order information, and partial payment card data. [The] compromised payment data includes customer names, the last four digits of card numbers, expiration dates, and even customer

fraud details" (collectively, "Private Information").[1]

2. This class action arises out of the recent targeted cyberattack against Ticketmaster that enabled a third party to access Defendants' computer systems and data, resulting in the compromise of highly sensitive Private Information (the "Data Breach").[2]

3. Due to the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses and value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm cause by the compromise of their Private Information.

PARTIES

4. Jane Doe is above the age of 19, and at all relevant times herein, a resident of the State of Alabama and as mother and next friend of Mary Doe.

5. Mary Doe is a minor, and at all relevant times herein, a resident of the State of Alabama.

6. Since 2018, Jane Doe and Mary Doe have been Defendants' customers and Ticketmaster account holders. Jane Doe provided her Private Information to

[1] Waqas, Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k, HACKREAD (Last accessed May 29, 2024), https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/.

[2] *Id*

Defendants, including her credit card, names of her minor daughter, and their shared address.

7. Jane Doe is deeply concerned by the Data Breach because she and her family frequently use Ticketmaster to purchase concert tickets, often on behalf of her minor daughter. This extreme concern continues to the present as both Jane and Mary Doe's information is readily available for cybercriminals to sell, buy, and exchange, on the Dark Web.

8. Since learning about the Data Breach, Plaintiffs anticipate needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiffs will need to review for fraudulent activity and closely monitor her financial information, and accounts.

9. Given the large-scale data leak, Plaintiffs also suffer as a result, a substantially increased risk of fraud, identity theft, and data misuse resulting from their Private Information being leaked on to the Dark Web and subjected to unauthorized third parties/criminals.

10. As such, Plaintiffs have a continuing interest in ensuring that their Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Defendant Ticketmaster, LLC.

11. Defendant Ticketmaster, LLC, is a wholly owned subsidiary of Defendant Live Nation Worldwide, Inc. headquartered in California with its Alabama office located at 4000 Eagle Point Corporate Drive, Birmingham, AL 35242.

12. Ticketmaster "operates as a ticket distribution company. [Ticketmaster] buys, transfers, and sells tickets for live music, sporting, arts, theater, and family events. Ticketmaster serves clients worldwide,"[3] including the state of Alabama.

13. Plaintiffs and Class Members are current and former customers of Ticketmaster.

14. Due to the nature of the services Ticketmaster provides, it receives and is entrusted with securely storing consumers' Private Information.

15. Ticketmaster through its privacy policy promised to provide confidentiality and adequate security for the data it collected from customers.

Defendant Live Nation Worldwide, Inc.

16. Defendant Live Nation Worldwide, Inc. is a Delaware corporation headquartered in California with its Alabama office located at 4000 Eagle Point Corporate Drive, Birmingham, AL 35242.

---

[3] *Ticketmaster LLC*, BLOOMBERG, https://www.bloomberg.com/profile/company/0009574D:US (Last accessed May 29, 2024).

17. Live Nation Worldwide is a publicly traded corporation with revenues totaling approximately $3.8 billion for the three months ended on March 31, 2024.[4]

18. Live Nation is "the largest live entertainment company in the world, connecting over 765 million fans across all of our concerts and ticketing platforms in 49 countries during 2023."[5]

19. Due to the nature of the services Live Nation provides, it receives and is entrusted with securely storing consumers' Private Information. Live Nation promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy.

JURISDICTION AND VENUE

20. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendants.

---

[4] *Form 10-Q Quarterly Report for Live Nation Entertainment, Inc.*, BAMSEC, https://www.bamsec.com/filing/133525824000071?cik=1335258 (last accessed May 29, 2024).
[5] *Form 10-K Annual Report for Live Nation Entertainment, Inc.*, BAMSEC, https://www.bamsec.com/filing/133525824000017?cik=1335258 (last accessed May 29, 2024).

21. Supplemental jurisdiction to adjudicate issues pertaining to Alabama state law is proper in this Court under 28 U.S.C. §1367.

22. Defendants routinely conducts business in Alabama, has sufficient minimum contacts in Alabama and has intentionally availed themselves of the laws, rights and benefits of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services.

23. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events giving rise to this action occurred in this jurisdiction. Moreover, Defendants are based in this jurisdiction, maintain Plaintiffs' and Class members' Private information in this jurisdiction, and has caused harm to Plaintiffs and Class Members in this jurisdiction.

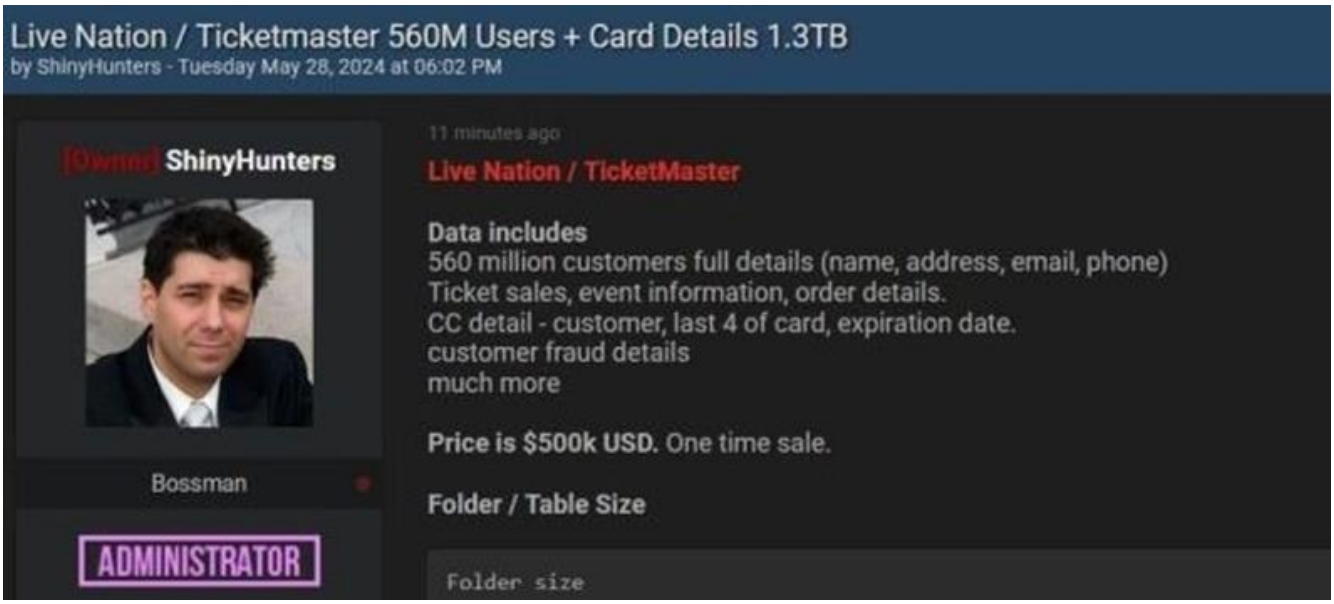
May 20, 2024 Ticketmaster Breach

24. On or around May 20, 2024, the Private Information of 560,000,000 Ticketmaster customers was compromised, and on May 27, 2024, listed for sale.[6]

25. The notorious hacker group known only by its alias "ShinyHunters", claimed that it had stolen 1.3 terabytes of personal data and is reportedly ready to sell, or has already sold, such information to nefarious dark web users for $500,000.00, as illustrated by their post on BreachForums, a dark-web marketplace

[6] Meera Navlakha, *Ticketmaster confirms massive hack. What you need to know.*, ABC NEWS (last accessed May 29, 2024), https://www.abc.net.au/news/2024-05-29/ticketmaster-hack-allegedlyshinyhunter-customers-data-leaked/103908614.

for stolen data.



26. Ticketmaster enabled an unauthorized third party to gain access to and obtain former and current Ticketmaster customers' Private Information from Ticketmaster's internal computer systems, resulting in this largescale breach.[7]

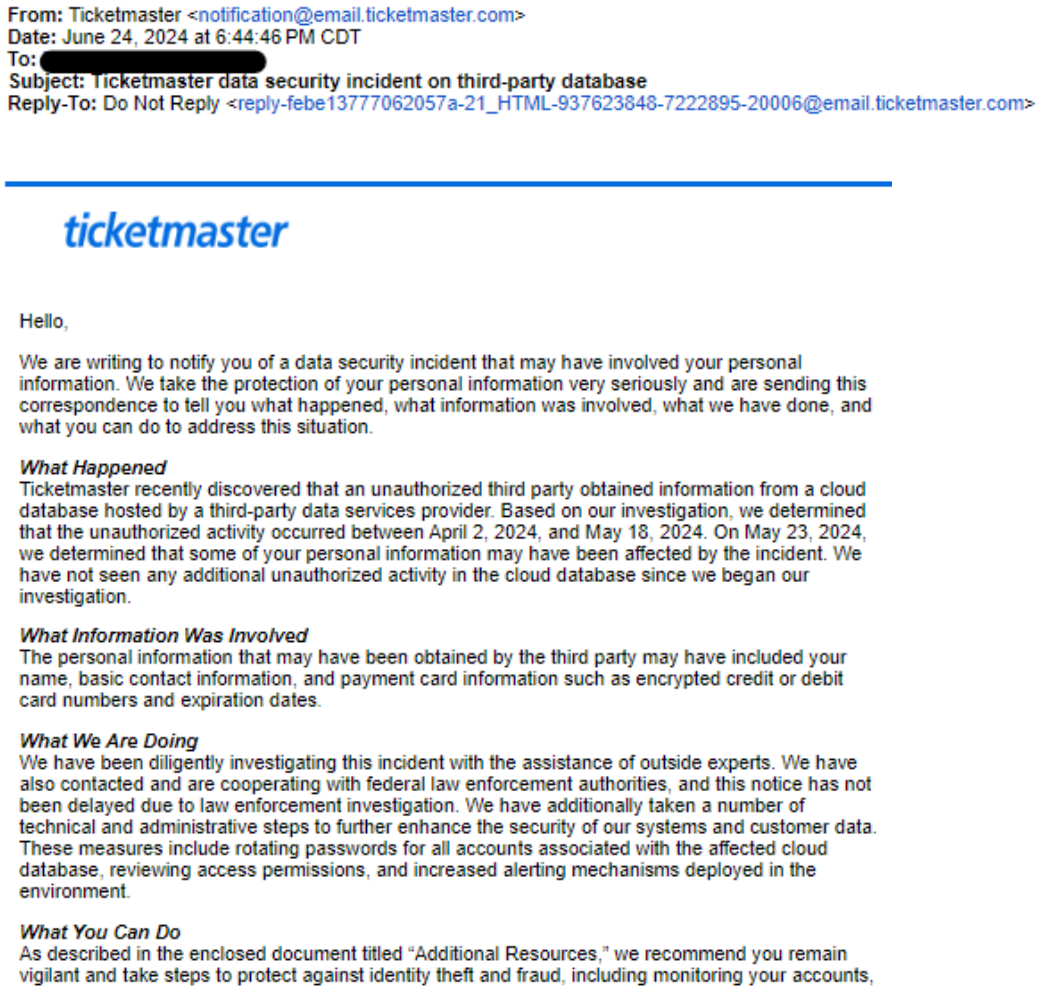
27. Defendants waited over a month to release a statement to notify its customers that their Private Information has been compromised and is likely in the hands of threat actors.

28. While Defendants claims to have discovered the breach as early as May 20, 2024, Defendants did not inform the SEC of the Data Breach until May 31, 2024,[8] and did not inform users until June 24, 2024.

29. Despite stating that the notice "was not delayed" there was a significant

[7] *Id*
[8] https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm (last accessed June 3, 2024)

gap between Defendants SEC Disclosure and notification to individual affected customers.



From: Ticketmaster <notification@email.ticketmaster.com>
Date: June 24, 2024 at 6:44:46 PM CDT
To: [redacted]
Subject: Ticketmaster data security incident on third-party database
Reply-To: Do Not Reply <reply-febe13777062057a-21_HTML-937623848-7222895-20006@email.ticketmaster.com>

ticketmaster

Hello,

We are writing to notify you of a data security incident that may have involved your personal information. We take the protection of your personal information very seriously and are sending this correspondence to tell you what happened, what information was involved, what we have done, and what you can do to address this situation.

What Happened
Ticketmaster recently discovered that an unauthorized third party obtained information from a cloud database hosted by a third-party data services provider. Based on our investigation, we determined that the unauthorized activity occurred between April 2, 2024, and May 18, 2024. On May 23, 2024, we determined that some of your personal information may have been affected by the incident. We have not seen any additional unauthorized activity in the cloud database since we began our investigation.

What Information Was Involved
The personal information that may have been obtained by the third party may have included your name, basic contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates.

What We Are Doing
We have been diligently investigating this incident with the assistance of outside experts. We have also contacted and are cooperating with federal law enforcement authorities, and this notice has not been delayed due to law enforcement investigation. We have additionally taken a number of technical and administrative steps to further enhance the security of our systems and customer data. These measures include rotating passwords for all accounts associated with the affected cloud database, reviewing access permissions, and increased alerting mechanisms deployed in the environment.

What You Can Do
As described in the enclosed document titled "Additional Resources," we recommend you remain vigilant and take steps to protect against identity theft and fraud, including monitoring your accounts,

30. Ticketmaster consumers were in the dark, unaware that their Private Information may be used to effectuate identity theft, phishing scams, and related cybercrimes.

31. Notably, most consumers, including Jane and Mary Doe, found out about the breach through media sources rather than the recent official disclosure.

32. The Data Breach was a direct result of Defendants' failure to implement

adequate and reasonable cybersecurity procedures and protocols, consistent with the industry standard, necessary to protect Private Information from the foreseeable threat of a cyberattack.

33. By acquiring Plaintiffs' and class members' Private Information for their own pecuniary benefit, Defendants assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class Members' Private Information against unauthorized access and disclosure.

34. Defendants also had a duty to adequately safeguard this Private Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "FTC Act").

35. Defendants breached those duties and disregarded the rights of Plaintiffs and the Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard consumers' Private Information; failing to take available and necessary steps to prevent unauthorized disclosure of data; and failing to follow applicable, required, and proper protocols, policies, and procedures regarding the encryption of data.

36. As a result of Defendants' inadequate security and breach of their duties and obligations, the Private Information of Plaintiffs and Class Members was

compromised through disclosure to an unauthorized criminal third party. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendants' conduct. These injuries include: (i) diminution in value and/or lost value of Private Information, a form of property that Defendants obtained from Plaintiffs and Class Members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' Private Information; (v) the continued and certain increased risk that the Private Information that remains in Defendants' possession is subject to further unauthorized disclosure for so long as Defendants fail to undertake proper measures to protect the Private Information; (vi) invasion of privacy and increased risk of fraud and identity theft; and (vii) theft of their Private Information and the resulting loss of privacy rights in that information. This action seeks to remedy these failings and their consequences. Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

37. Despite having been accessed and exfiltrated by unauthorized criminal

actors, Plaintiffs' and Class Members' sensitive and confidential Private Information remains in the possession of Defendants. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft. The aggregate data compromised in the Data Breach, taken as a whole, increases the risk of harm, making identity theft a likely outcome.

38. Defendants disregarded the rights of Plaintiffs and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

39. In addition, Defendants failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored these electronic systems, Defendants may have discovered the intrusion sooner or prevented it altogether.

40. The security of Plaintiffs' and Class Members' identities is now at substantial risk because of Defendants' wrongful conduct as the Private Information that Defendants collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

41. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiffs and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

42. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. And because they exposed other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

43. Plaintiffs, on behalf of themselves and all other Class Members, bring claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

CLASS ACTION ALLEGATIONS

A. The Data Breach, and Defendants Unsecure Data Management

44. On May 28, 2024, threat actors posted that 1.4 terabytes of Private Information were available for purchase on the hacking website Breach Forums.[9]

45. The hacking group ShinyHunters, stole and subsequently offered the Plaintiffs' and Class Members' 1.4 terabytes of Private Information for $500,000.

46. Such data includes, according to the hackers' forum post, "560 million customers [*sic*] full details (name, address, email, phone) – Ticket sales, event information, order details – CC [credit card] detail [*sic*] – customer, last 4 of card, expiration date. Customer fraud details – much more."[10]

47. Prior to the Data Breach in May 2024, Plaintiffs and Class Members had provided their Private Information to Ticketmaster with the reasonable expectation and mutual understanding that Ticketmaster would comply with its obligations to keep such information confidential and secure from unauthorized access. In particular, Plaintiffs and Class Members provided their names, emails, phone numbers, location data and credit card information to Ticketmaster in order to register for an account and purchase event tickets on Ticketmaster.com.

48. PII is a valuable property right.[11] "Firms are now able to attain

---

Waqas, *supra* note 1.

[10] *Id*

[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26-38 (last accessed May 2015),

significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[12] It is estimated that American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[13] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years. Indeed, the threat actor who compromised Defendants' systems is seeking a one-time payment of half a million dollars in exchange for this Private Information.

49. Plaintiffs and the Class's Private Information exposed in the Data Breach has been exposed on the Dark Web.

50. Ticketmaster promised consumers it would keep their data secure and private. Data security is purportedly a critical component of Ticketmaster's business model. On a section of its website, Ticketmaster confidently asserts the following statements:

---

https://www.researchgate.net/publication/283668023 The Value of Personal Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[12] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD No. 220 (last accessed Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[13] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (last accessed Dec. 5, 2018), https://www.iab.com/news/2018-state -of-data-report/.

> "We're always taking steps to make sure your information is protected and deleted securely," "[we] have security measure in place to protect your information,"[14] and "[the] security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."[15]

51. On its website, Ticketmaster maintains an "Our Commitments" section, including "Security & Confidentiality" as one of "10 commitments that drive [Ticketmaster's] privacy program, globally."[16]

52. Contrary to Ticketmaster's various express assurances that it would take reasonable measures to safeguard the sensitive information entrusted to it, an "unauthorized" person or persons was able to access its network servers.

53. To date, Ticketmaster has not disclosed complete specifics of the attack, such as whether ransomware has been used.

54. As such, Ticketmaster, and its parent company Live Nation, have failed to secure the PII of the individuals that provided their sensitive information. Defendants failed to take appropriate steps to protect the PII of Plaintiffs and other Class Members from being disclosed.

---

[14] *Privacy Policy*, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last accessed May 29, 2024).
[15] *Our Commitments*, TICKETMASTER, https://privacy.ticketmaster.com/en/our-commitments (last accessed May 29, 2024).
[16] *Id*

B. Defendants Failed to Comply with FTC Guidelines

55. Defendants were prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

56. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17]

[17] *Protecting Personal Information: A Guide of Business,* FEDERAL TRADE COMMISSION (last accessed Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g.*, In the Matter of LabMD, Inc., A

[18] *Id*

Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

61. Defendants failed to properly implement basic data security practices, allowing for this attack to occur, victimizing millions of people.

62. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. Defendants were at all times fully aware of the obligation to protect the Private Information of customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

C. Plaintiffs and the Class Have Suffered Injury as a Result of Defendants' Data Mismanagement

64. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiffs and Class Members' Private Information has been and are now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiffs and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

65. Plaintiffs and Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

66. Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim for cybercrimes for years to come.

67. As a result of Private Information's real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

68. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian reports that a stolen

[19] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (last accessed Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs//.

credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

69. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

70. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

71. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[22]

---

[20] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web,* EXPERIAN (last accessed Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[21] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study,* 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1 (Last accessed May 2, 2024).

[22] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware,* LAW360 (Nov. 18, 2019), accessible at https://www.law360.com/articles/1220974 (Last accessed May 2, 2024)

72. Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

73. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendants' conduct. Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by its exposure in the Data Breach.

74. As a result of Defendants' failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

75. Plaintiffs and members of the Class suffered actual injury from having Private Information compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of property that

Defendants obtained from Plaintiffs; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

76. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm.

77. Plaintiffs, individually and on behalf of all other similarly situated individuals, allege claims in negligence, negligence per se, breach of implied contract, unjust enrichment, violations of the of the Alabama Data Breach Notification Act and the Alabama Deceptive Trade Practices Act.

CLASS ACTION ALLEGATIONS

78. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

79. Plaintiffs propose the following Class and Subclass definitions, subject to amendment(s) as appropriate:

Nationwide Class: All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach. ("the Class").

Alabama Subclass: All individuals identified by Defendants (or their agents or affiliates) as being those persons residing in Alabama impacted by the Data Breach. (the "Alabama Subclass").

80. Collectively, the Class and Alabama Subclass are referred to as the Classes.

81. Excluded from the Classes are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

82. Plaintiffs reserve the right to amend or modify the Class or Subclass definitions as this case progresses.

83. **Numerosity:** Upon information and belief, the members of the Class are so numerous that joinder of all of them is impracticable.

84. **Predominance of Common Questions:** There exist questions of law and fact common to the Class, which predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants were subject to (and breached) the Alabama Breach Notification Act of 2018.

g. Whether Defendants were subject to (and breached) the Alabama Deceptive Trade Practices Act.

h. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

i. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

j. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants' acts breached an implied contract they formed with Plaintiffs and the Class Members;

m. Whether Defendants were unjustly enriched to the detriment of Plaintiffs and the Class;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

85. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

86. **Adequacy:** Plaintiffs are adequate representatives for the Class because their interests do not conflict with the interests of the Class that they seek to represent. Plaintiffs have retained counsel competent and highly experienced in complex class action litigation counsel intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their experienced counsel.

87. **Superiority:** A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and members of the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Defendants. Even if Class Members could afford such individual

litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, inter alia, the records (including databases, e-mails, dealership records and files, etc.) Defendants maintain regarding their consumers.

88. Defendants have acted on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

ALABAMA LAW SHOULD BE APPLIED TO THE NATIONWIDE CLASS

89. The State of Alabama has a significant interest in regulating the conduct of businesses operating within its borders. Alabama seeks to protect the rights and interests of all Alabama residents and citizens of the United States against a company with a registered agent in, and doing business in Alabama.

90. Defendants conduct substantial business in Alabama, such that Alabama has an interest in regulating Defendants' conduct under its laws.

91. Each Defendant's decision to conduct substantial business in Alabama and avail itself of Alabama's laws, renders the application of Alabama law to the

claims herein constitutionally permissible.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

92. Plaintiffs reallege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

93. Defendants owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, or control.

94. Defendants knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class Members' Private Information and the importance of maintaining secure systems. Defendants knew, or should have known, of the vast uptick in data breaches in recent years. Defendants had a duty to protect the Private Information of Plaintiffs and Class Members.

95. Given the nature of Defendants' business, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendants had a duty to prevent.

96. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information

by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiffs' and Class Members' Private Information.

97. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

98. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and the Class Members, their Private Information would not have been compromised.

99. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for

protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well- established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE
(On Behalf of the Plaintiffs and the Nationwide Class)

100. Plaintiffs reallege and incorporate by reference paragraphs 1 - 90 as if fully set forth herein.

101. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Private Information.

102. Defendants violated Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of

Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

103. Defendants' violations of Security Rules and Section 5 of the FTCA constitute negligence per se.

104. Plaintiffs and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

105. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

106. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

107. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendants' violations of Security Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the

form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class)

108. Plaintiffs reallege and incorporate by reference paragraphs 1 - 90 as if fully set forth herein.

109. Plaintiffs and Class Members either directly or indirectly gave Defendants their Private Information in confidence, believing that Defendants would protect that information. Plaintiffs and Class Members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class Members' Private Information created a fiduciary relationship between Defendants and Plaintiffs and Class Members. Considering this relationship, Defendants must act primarily for the benefit of their consumers, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information.

110. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' Private Information, failing to safeguard the Private Information of Plaintiffs and Class Members it collected.

111. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
VIOLATION OF ALABAMA DATA BREACH NOTIFICATION ACT OF 2018
(On Behalf of Plaintiffs and the Nationwide Class)

112. Plaintiffs reallege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

113. The Alabama Data Breach Notification Act requires that companies that own or license computerized data including sensitive personally identifiable information provide notice to Alabama residents of any data breach.

114. Defendants violated the Alabama Data Breach Notification Act by failing to disclose the Data Breach to Plaintiffs and other Class Members in a timely and accurate manner.

115. As a result of Defendants' violations of the Alabama Data Breach Notification Act, Plaintiffs and Class Members have suffered damages and seek statutory penalties, compensatory damages, and equitable relief.

COUNT V
VIOLATION OF ALABAMA DECEPTIVE TRADE PRACTICES ACT

116. Plaintiffs reallege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

117. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1, et seq.

118. Defendants' deceptive, unfair, and unlawful trade acts or practices include: a. Failing to maintain adequate computer systems and data security practices to safeguard Private Information; b. Failing to disclose that its computer

systems and data security practices were inadequate to safeguard Private Information from theft; c. Failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members; d. Continued acceptance of Private Information and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and e. Continued acceptance of Private Information and storage of other personal information after Defendants knew or should have known of the Data Breach and before they allegedly remediated the Data Breach.

119. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

120. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information

which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or statutory damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

121. Plaintiffs reallege and incorporate by reference paragraphs 1 - 90 as if fully set forth herein. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

122. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for services.

123. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class Members' Private Information.

124. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures

that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

125. Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

126. Defendants should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it because of the conduct and Data Breach alleged herein.

COUNT VII
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

127. Plaintiffs realleges and incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

128. Defendants required Plaintiffs and Class Members to provide or authorize the transfer of their Private Information for Defendants to provide services. In exchange, Defendants entered implied contracts with Plaintiffs and Class Members in which Defendants agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' Private Information and to timely notify them in the event of a data breach.

129. Plaintiffs and Class Members would not have provided their Private Information to Defendants had they known that Defendants would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

130. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

131. Defendants breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

132. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendants' breach of its implied contracts with Plaintiffs and Class Members.

COUNT VIII
INVASION OF PRIVACY
(*On behalf of Plaintiffs and the Nationwide Class*)

133. Plaintiffs realleges and incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

134. Representative Plaintiffs and Class Members had a legitimate expectation of privacy in their PII and SSN and were entitled to the protection of this information against disclosure to unauthorized third parties.

135. Defendant owed a duty to Representative Plaintiffs and Class Members to keep their PII and SSN confidential.

136. Defendant failed to protect and released to unknown and unauthorized third parties the PII and SSN of Representative Plaintiffs and Class Members.

137. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and SSN of Representative Plaintiffs and Class Members, by way of Defendant's failure to protect the PII and SSN.

138. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and SSN of Representative Plaintiffs and Class Members is highly offensive to a reasonable person.

139. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Representative Plaintiffs and Class Members disclosed their PII and SSN to Defendant as part of obtaining services from Defendant, but privately with an intention that the PII and SSN would be kept confidential and would be protected from unauthorized disclosure. Representative Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

140. The Data Breach constitutes an intentional interference with Representative Plaintiffs' and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

141. Defendant acted with a knowing state of mind when it permitted the

Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

142. Because Defendant acted with this knowing state of mind, it had notice and knew its inadequate and insufficient information security practices would cause injury and harm to Representative Plaintiffs and Class Members.

143. As a proximate result of the above acts and omissions of Defendants, the PII and SSN of Representative Plaintiffs and Class Members was disclosed to third parties without authorization, causing Representative Plaintiffs and Class Members to suffer damages.

144. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Representative Plaintiffs and Class Members in that the PII and SSN maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Representative Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Representative Plaintiffs and/or Class Members.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, on behalf of herself and each member of the proposed National Class and the Alabama Subclass, respectfully requests that the Court enter judgment in their favor and for the following specific

relief against Defendant as follows:

1. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

2. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information;

3. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

4. For an order requiring Defendants to pay for credit monitoring services for Plaintiffs and the Class of a duration to be determined at trial;

5. For an award of punitive damages, as allowable by law;

6. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

7. Pre- and post-judgment interest on any amounts awarded; and

8. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Representative Plaintiffs, individually and on behalf of the Plaintiff Class and/or Subclass, hereby demands a trial by jury for all issues triable by jury.

Submitted this the 19 day of July, 2024.

/s/ *Eric J. Artrip*
Eric J. Artrip ASB-9673-I68E
MASTANDO & ARTRIP, LLC
301 Holmes Ave., NE, Ste. 100
Huntsville, Alabama 35801
Phone: (256) 532-2222
Fax: (256) 513-7489
artrip@mastandoartrip.com

/s/ *Brent Irby*
Brent Irby ASB-2773-R79R
IRBY LAW LLC
2201 Arlington Avenue South
Birmingham AL 35205
P: 205-936-8281
brent@irbylaw.net

DEFENDANTS TO BE SERVED VIA CERFIFED MAIL:

Live Nation Worldwide, Inc.
4000 Eagle Point Corporate Drive
Birmingham, AL 35242

Ticket Master, LLC
4000 Eagle Point Corporate Drive
Birmingham, AL 35242